(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－110543
（P2003－110543A）
(43)公開日　平成15年４月11日(2003.4.11)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)	
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ	12/28	３００Ａ	５Ｊ１０４
12/28	３００		9/00	６０１Ｄ	５Ｋ０３３

審査請求　有　　請求項の数10　ＯＬ　（全　８　頁）

(21)出願番号　特願2001－298631(P2001－298631)

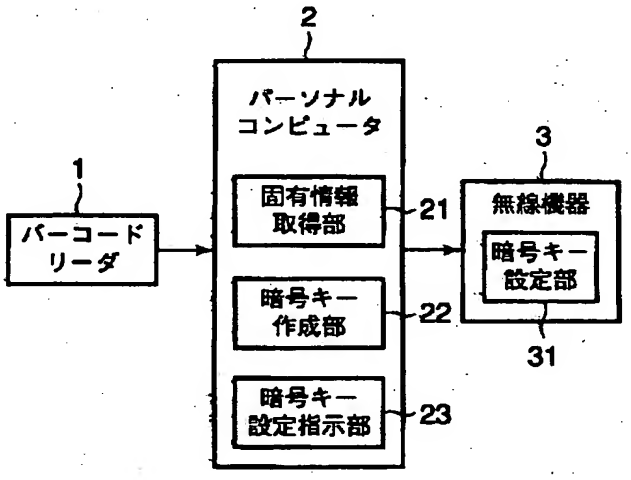
(22)出願日　平成13年９月27日(2001.9.27)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　波多野　健
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(72)発明者　鍛治　孝一
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

Ｆターム(参考)　5J104 AA16 EA26 NA02
5K033 AA08 DA17 EC01

(54)【発明の名称】　暗号キー設定システム、無線通信装置および暗号キー設定方法

(57)【要約】
【課題】暗号キーが初期設定のままの状態で利用されてもセキュリティを維持することを実現する暗号キー設定システムを提供する。
【解決手段】無線機器３は、この暗号キー設定システムで処理対象とする、たとえば製造・販売元の出荷製品であり、パーソナルコンピュータ２の固定情報取得部２１は、バーコードリーダ１を用いて無線機器３に固有の情報、たとえば製造番号やＭＡＣアドレスなどを取得する。また、暗号キー作成部２２は、この固定情報取得部２１により取得された情報を利用して、無線機器３が無線通信時に用いる暗号キーを作成する。そして、暗号キー設定指示部２３は、この暗号キー作成部２２が作成した暗号キーを設定させるための命令を無線機器３に向けて発行する。一方、この命令を受け取った無線機器３では、暗号キー設定部３１が、この暗号キーの設定を実行する。



1

【特許請求の範囲】
【請求項１】　無線通信装置が有する機器固有情報を取得する固有情報取得手段と、
前記固有情報取得手段により取得された機器固有情報を用いて前記無線通信装置が無線通信を行う際のデータ暗号キーを作成する暗号キー作成手段と、
前記暗号キー作成手段により作成された暗号キーを前記無線通信装置に設定する設定手段とを具備することを特徴とする暗号キー設定システム。
【請求項２】　前記固有情報取得手段は、前記無線通信装置の製造番号を取得することを特徴とする請求項１記載の暗号キー設定システム。
【請求項３】　前記固有情報取得手段は、前記無線通信装置に割り当てられたＭＡＣアドレスを取得することを特徴とする請求項１記載の暗号キー設定システム。
【請求項４】　前記固有情報取得手段は、バーコードリーダにより前記機器固有情報を読み取ることを特徴とする請求項１、２または３記載の暗号キー設定システム。
【請求項５】　前記暗号キー作成手段は、ＥＳＳ－ＩＤを作成することを特徴とする請求項１、２、３または４記載の暗号キー設定システム。
【請求項６】　前記暗号キー作成手段は、ＷＥＰキーを作成することを特徴とする請求項１、２、３または４記載の暗号キー設定システム。
【請求項７】　前記設定手段により前記無線通信装置に設定した暗号キーを当該システムが動作する装置に設定する第２の設定手段を具備することを特徴とする請求項１、２、３、４、５または６記載の暗号キー設定システム。
【請求項８】　無線通信を行う際のデータ暗号キーの初期設定指示を入力する入力手段と、
前記入力手段により前記初期設定指示が入力されたときに、自装置が有する機器固有情報を取得する固有情報取得手段と、
前記固有情報取得手段により取得された機器固有情報を用いて暗号キーを作成する暗号キー作成手段と、
前記暗号キー作成手段により作成された暗号キーを自装置に設定する設定手段とを具備することを特徴とする無線通信装置。
【請求項９】　無線通信装置が有する機器固有情報を取得する固有情報取得ステップと、
前記固有情報取得ステップにより取得された機器固有情報を用いて前記無線通信装置が無線通信を行う際のデータ暗号キーを作成する暗号キー作成ステップと、
前記暗号キー作成ステップにより作成された暗号キーを前記無線通信装置に設定する設定ステップとを具備することを特徴とする暗号キー設定方法。
【請求項１０】　無線通信を行う際のデータ暗号キーの初期設定指示を入力する入力ステップと、
前記入力ステップにより前記初期設定指示が入力されたときに、自装置が有する機器固有情報を取得する固有情報取得ステップと、
前記固有情報取得ステップにより取得された機器固有情報を用いて暗号キーを作成する暗号キー作成ステップと、
前記暗号キー作成ステップにより作成された暗号キーを自装置に設定する暗号キー設定ステップとを具備することを特徴とする暗号キー設定方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、たとえば無線ＬＡＮアクセスポイント等の無線通信装置に暗号キーを設定するための暗号キー設定システム、自装置の暗号キーを設定する機能を有する無線通信装置および暗号キー設定方法に係り、特に、暗号キーが初期設定のままの状態で利用されてもセキュリティを維持することを実現する暗号キー設定システム、無線通信装置および無線通信方法に関する。
【０００２】
【従来の技術】近年、無線ＬＡＮ（IEEE802.11b）やBluetoothなどといった、パーソナルエリアの無線通信システムが注目されている。また、この種の無線通信システムでは、無線の特性上、電波を傍受されるおそれがあることや、ネットワーク環境に誰でも接続可能となるおそれがあることから、セキュリティの維持のために、暗号キーによって接続認証を行う機能をもっている。
【０００３】そこで、ユーザは、互いに無線通信を行わせたい複数の無線通信装置間で同期させて、同一の暗号キーを各々設定するなどといった作業を行っていた。
【０００４】たとえば、IEEE802.11におけるセキュリティとしては、ＷＥＰ(Wired Equivalent Privacy)キーと呼ばれる４０ビットの暗号化されたコードを用いることで、同じＷＥＰコードを持つ無線機器以外からの接続を許可しないようにするものや、ＳＳ－ＩＤ(Service Set ID)と呼ばれる無線機器間でのグループ設定を行うものが知られている。
【０００５】
【発明が解決しようとする課題】しかしながら、ユーザの中には、セキュリティ維持の意識が低い者も少なからず見受けられ、暗号キーを考慮することなく、無線通信装置を使い始めてしまうユーザも存在するのが現状である。
【０００６】一方、無線通信装置の製造・販売元では、ユーザによる暗号キーの設定を想定しているため、一般的には、暗号キーを設定せずに、または、所定の暗号キーを暫定的に設定して出荷している。したがって、ユーザが出荷時の初期設定のままの状態で無線通信装置を使用すると、無関係な相手との通信が行われてしまうといった事態が発生しうる。つまり、たとえば無線ＬＡＮを構築するためのアクセスポイントがこのような状態で使

用されると、不正なユーザからの侵入を許すことにもなってしまう。

【０００７】この発明は、このような事情を考慮してなされたものであり、暗号キーが初期設定のままの状態で利用されてもセキュリティを維持することを実現する暗号キー設定システム、無線通信装置および無線通信方法を提供することを目的とする。

【０００８】

【課題を解決するための手段】前述した目的を達成するために、この発明の暗号キー設定システムは、無線通信装置が有する機器固有情報を取得する固有情報取得手段と、前記固有情報取得手段により取得された機器固有情報を用いて前記無線通信装置が無線通信を行う際のデータ暗号キーを作成する暗号キー作成手段と、前記暗号キー作成手段により作成された暗号キーを前記無線通信装置に設定する設定手段とを具備することを特徴とする。

【０００９】この暗号キー設定システムにおいては、たとえば製造・販売元からの出荷時などにおいて、製造番号やＭＡＣ（Media Access Control）アドレスなど、無線通信装置に固有の情報を取得し、その固有情報から暗号キーを作成して、それぞれの無線通信装置に設定する。

【００１０】すなわち、この暗号キー設定システムでは、製品１つ１つに固有の暗号キーを割り当てるといった非常に手間がかかる、従来であれば非現実的であった作業を自動化することにより、ユーザが出荷時と同じ初期設定のままの状態で無線通信装置を使い始めたとしても、無関係な相手との通信が行われてしまうといった事態を防止し、セキュリティを維持することを実現する。

【００１１】

【発明の実施の形態】以下、図面を参照してこの発明の実施形態を説明する。

【００１２】（第１実施形態）まず、この発明の第１実施形態について説明する。

【００１３】図１は、この第１実施形態に係る暗号キー設定システムの全体図である。図１に示すように、この暗号キー設定システムでは、バーコードリーダ１とパーソナルコンピュータ２とが接続され、さらに、このパーソナルコンピュータ２と無線機器３とが接続される。この無線機器３は、たとえば無線ＬＡＮアクセスポイントなどであり、この暗号キー設定システムで処理対象とする、たとえば製造・販売元の出荷製品である。

【００１４】また、パーソナルコンピュータ２は、固有情報取得部２１、暗号キー作成部２２および暗号キー設定指示部２３を備え、無線機器３は、暗号キー設定部３１を備えている。

【００１５】図２は、このパーソナルコンピュータ２の機器構成を示す図である。このパーソナルコンピュータ２は、たとえばデスクトップタイプやノートブックタイプのコンピュータであり、図２に示すように、ＣＰＵ１０１、ＤＲＡＭ１０２、ＨＤＤ１０３、表示コントローラ１０４、キーボードコントローラ１０５およびＩ／Ｏコントローラ１０６を有している。

【００１６】ＣＰＵ１０１は、このパーソナルコンピュータ２の動作を統合的に制御するものであり、ＤＲＡＭ１０２に格納されたユーティリティソフトウェアａを含む各種プログラムの記述にしたがって各部の動作を制御する。また、ユーティリティソフトウェアａは、このパーソナルコンピュータ２を暗号キー設定システムとして動作させるためのプログラムであり、ＨＤＤ１０３から適宜ロードされてＤＲＡＭ１０２に格納される。そして、図１で示した固有情報取得部２１、暗号キー作成部２２および暗号キー設定指示部２３は、このユーティリティソフトウェアａによって実現される。

【００１７】ＤＲＡＭ１０２は、このパーソナルコンピュータ２の主記憶となるメモリデバイスであり、ユーティリティソフトウェアａを含む各種プログラムや、これらのプログラムから入出力される各種データを格納する。また、ＨＤＤ１０３は、このパーソナルコンピュータ２の外部記憶となるメモリデバイスであり、ＤＲＡＭ１０２の２次記憶として各種プログラムおよび各種データを大量に格納する。

【００１８】表示コントローラ１０４は、このパーソナルコンピュータ２におけるユーザインタフェースのアウトプットを司るものであり、ＣＰＵ１０１が作成した表示データをＣＲＴやＬＣＤに表示する。一方、キーボードコントローラ１０５は、このパーソナルコンピュータ２におけるユーザインタフェースのインプットを司るものであり、キーボードやマウスの操作を数値化してＣＰＵ１０１に引き渡す。

【００１９】また、Ｉ／Ｏコントローラ１０６は、外部機器との間の有線による通信を制御するものであり、バーコードリーダ１や無線機器３とは、このＩ／Ｏコントローラ１０６が備えるインタフェースコネクタを介して接続される。

【００２０】図３は、無線機器３の機器構成を示す図である。この無線機器３は、無線ＬＡＮ（IEEE802.11b）規格に準拠した無線通信を行うものであり、図３に示すように、ＣＰＵ２０１、ＥＥＰＲＯＭ２０２、フラッシュメモリ２０３、ＤＲＡＭ２０４、無線通信部２０５、表示コントローラ２０６およびＩ／Ｏコントローラ２０７を有している。

【００２１】IEEE802.11b方式では、ＩＳＭ（Industrial Scientific Medical）バンドと呼ばれる２．４ＧＨｚ帯を使用して無線通信を行ない、送受信信号の変調方式として、直接拡散方式のスペクトル拡散通信（ＤＳＳＳ：Direct Sequence Spred Spectrum）を用いている。さらに、２．４ＧＨｚ帯（２．４０００～２．４８３５ＧＨｚ）を１４のチャネル（国によっては使用チャネルが制限される）に分割して使用する。各チャネルの占有

帯域は、各チャネルの中心周波数から±１１ＭＨｚの２２ＭＨｚである。この通信チャネルは、無線通信を行う機器間で同一のチャネルを使用するように設定される。

【００２２】ＣＰＵ２０１は、この無線機器３の動作を統合的に制御するものであり、フラッシュメモリ２０３に格納された暗号キー設定プログラムｃを含む各種プログラムの記述にしたがって各部の動作を制御する。また、暗号キー設定プログラムｃは、ＥＥＰＲＯＭ２０２に格納される、無線通信時の接続認証に利用される暗号キーｂを設定するためのプログラムである。この暗号キー設定システムでは、たとえばIEEE802.11bで規定されたＷＥＰ（Wired Equivalent Privacy）キーやＥＳＳ－ＩＤ（Extended Service Set-ID）を暗号キーｂとして取り扱う。そして、図１で示した暗号キー設定部３１は、この暗号キー設定プログラムｃによって実現される。

【００２３】ＥＥＰＲＯＭ２０２は、暗号キーｂを含む各種設定情報を格納するメモリデバイスであり、フラッシュメモリ２０３は、暗号キー設定プログラムｃを含む各種プログラムを格納するメモリデバイスである。また、ＤＲＡＭ２０４は、ＣＰＵ２０１の作業領域となるメモリデバイスである。

【００２４】無線通信部２０５は、他の無線機器との間の無線による通信を制御するものであり、IEEE802.11bの無線機能を制御するベースバンドＬＳＩ、このベースバンドＬＳＩが実行するプログラムを格納するフラッシュメモリ、アンテナおよびベースバンドＬＳＩとアンテナとの間における高周波信号の制御を行なうＲＦ部を具備している。

【００２５】表示コントローラ２０６は、この無線機器３におけるユーザインタフェースのアウトプットを司るものであり、ＣＰＵ２０１が作成した表示データをＬＣＤに表示する。一方、Ｉ／Ｏコントローラ２０７は、この無線機器３におけるユーザインタフェースのインプットを司るものであり、各種ボタンの押下をＣＰＵ２０１に通知する。また、このＩ／Ｏコントローラ２０７は、外部機器との間の有線による通信の制御も行い、パーソナルコンピュータ２とは、このＩ／Ｏコントローラ２０７が備えるインタフェースコネクタを介して接続される。

【００２６】次に、このような機器構成をもつこの暗号キー設定システムの動作について説明する。図４は、この暗号キー設定システムの動作手順を示すフローチャートである。

【００２７】たとえば無線機器３の製造・販売元で、その出荷時に無線機器３の暗号キーｂを設定する場合、まず、オペレータが、パーソナルコンピュータ２のユーティリティソフトウェアａを起動する（ステップＡ１）。

【００２８】ユーティリティソフトウェアａが起動されると、固定情報取得部２１、暗号キー作成部２２および暗号キー設定指示部２３が作動するので、オペレータは、バーコード化されて受注伝票などに印刷された無線機器３の製造番号やＭＡＣアドレスなどをバーコードリーダ１で読み取る。このバーコードリーダ１で読み取られた製造番号やＭＡＣアドレスなどは、無線機器３に固有の情報として固有情報取得部２１が取得する（ステップＡ２）。

【００２９】また、固有情報取得部２１は、この取得した情報を暗号キー作成部２２に転送する。一方、暗号キー作成部２２は、この転送された情報を利用して、無線機器３が無線通信時に用いる暗号キーを作成する（ステップＡ３）。この暗号キー作成部２２による暗号キーの作成は、たとえば製造番号またはＭＡＣアドレスの一部または全部に所定の手順でスクランブルをかけるなど、ある規則性を持たせることができれば、つまり再現できればどのような方法であってもよい。また、たとえば桁合わせなどを行うのみで、この製造番号またはＭＡＣアドレスの一部または全部をそのまま暗号キーとしても構わない。

【００３０】そして、暗号キー設定指示部２３は、この暗号キー作成部２２が作成した暗号キーを設定させるための命令を、Ｉ／Ｏコントローラ１０６を介して無線機器３に向けて発行する（ステップＡ４）。一方、この命令をＩ／Ｏコントローラ２０７を介して受け取った無線機器３では、暗号キー設定部３１が、この暗号キーをＥＥＰＲＯＭ２０２に格納する（ステップＡ５）。

【００３１】以降、オペレータは、パーソナルコンピュータ２と接続する無線機器３を交換していきながら、前述の処理を繰り返す。

【００３２】このように、この実施形態の暗号キー設定システムでは、各無線機器３に固有の暗号キーを簡単に設定することを可能としており、ユーザが出荷時と同じ初期設定のままの状態で無線通信装置を使い始めたとしても、無関係な相手との通信が行われてしまうといった事態を防止し、セキュリティを維持することを実現する。

【００３３】（第２実施形態）次に、この発明の第２実施形態について説明する。

【００３４】図５は、この第２実施形態に係る暗号キー設定システムの全体図である。前述した第１実施形態の暗号キー設定システムとこの第２実施形態の暗号キー設定システムとの違いは、図５に示すように、無線機器３自身が、暗号キー作成部３２を備える点にある。この暗号キー作成部３２は、パーソナルコンピュータ２から暗号キーを設定する旨の命令が発行されたときに、たとえば自装置に割り当てられたＭＡＣアドレスをＥＥＰＲＯＭ２０２から読み出し、この読み出したＭＡＣアドレスを利用して、自機器が無線通信時に用いる暗号キーを作成する。

【００３５】これに伴い、パーソナルコンピュータ２で

は、バーコード１との接続と固有情報取得部２１および暗号キー作成部２２とが不要となり、また、暗号キー設定指示部２３は、（暗号キーの転送を伴わない）暗号キーを設定する旨の命令を無線機器３に発行する機能のみを備えればよい。

【００３６】図６は、この第２実施形態の暗号キー設定システムの動作手順を示すフローチャートである。

【００３７】たとえば無線機器３の製造・販売元等のオペレータは、まず、パーソナルコンピュータ２のユーティリティソフトウェアａを起動する（ステップＢ１）。ユーティリティソフトウェアａが起動されると、暗号キー設定指示部２３が作動するので、オペレータは、この暗号キー設定指示部２３に、暗号キーを設定させるための命令を、Ｉ／Ｏコントローラ１０６を介して無線機器３に向けて発行させる（ステップＢ２）。

【００３８】一方、この命令をＩ／Ｏコントローラ２０７を介して受け取った無線機器３では、暗号キー作成部３２が、たとえば自装置に割り当てられたＭＡＣアドレスから無線通信時に用いる暗号キーを作成する（ステップＢ３）。そして、暗号キー設定部３１が、この暗号キー作成部３２により作成された暗号キーをＥＥＰＲＯＭ２０２に格納する（ステップＢ４）。

【００３９】以降、オペレータは、パーソナルコンピュータ２と接続する無線機器３を交換していきながら、前述の処理を繰り返す。

【００４０】このように、この実施形態の暗号キー設定システムも、各無線機器３に固有の暗号キーを簡単に設定することを可能とし、ユーザが出荷時と同じ初期設定のままの状態で無線通信装置を使い始めたとしても、無関係な相手との通信が行われてしまうといった事態を防止し、セキュリティを維持することを実現する。

【００４１】なお、ここでは、パーソナルコンピュータ２からの命令に応じて、暗号キー作成部３２および暗号キー設定部３１が作動する例を示したが、この暗号キーを設定する旨を指示するためのボタンを無線機器３に設け、このボタンの操作を無線機器３のＩ／Ｏコントローラ２０７が検知したときに、暗号キー作成部３２および暗号キー設定部３１が作動するようにしてもよい。この場合には、無線機器３単体で暗号キーの設定を行うことができ、また、オペレータは、無線機器３に設けられた所定のボタンを操作すればよいことになる。

【００４２】（第３実施形態）次に、この発明の第３実施形態について説明する。

【００４３】図７は、この第３実施形態に係る暗号キー設定システムの全体図である。前述した第１実施形態の暗号キー設定システムとこの第３実施形態の暗号キー設定システムとの違いは、図７に示すように、パーソナルコンピュータ２側にも、暗号キー設定部２４を設けた点にある。この暗号キー設定部２４は、暗号キー設定指示部２３から無線機器３に向けて暗号キーを設定する旨の命令が発行されたときに、その暗号キーをパーソナルコンピュータ２にも設定する。

【００４４】この第３実施形態の暗号キー設定システムでは、パーソナルコンピュータ２も処理対象、つまり、たとえば製造・販売元の出荷製品とし、かつ、このパーソナルコンピュータ２と無線機器３とがセットで出荷されて互いに無線通信を行うことを想定している。そして、このように、パーソナルコンピュータ２と無線機器３とが同期をとって同一の暗号キーを設定しなければならない場合のために、この第３実施形態の暗号キー設定システムは、これらを自動的に実行する仕組みを提供する。

【００４５】図８は、この第３実施形態の暗号キー設定システムの動作手順を示すフローチャートである。

【００４６】たとえば無線機器３の製造・販売元等のオペレータは、まず、パーソナルコンピュータ２のユーティリティソフトウェアａを起動する（ステップＣ１）。ユーティリティソフトウェアａが起動されると、固定情報取得部２１、暗号キー作成部２２、暗号キー設定指示部２３および暗号キー設定部２４が作動するので、オペレータは、バーコード化されて受注伝票などに印刷された無線機器３の製造番号やＭＡＣアドレスなどをバーコードリーダ１で読み取る。このバーコードリーダ１で読み取られた製造番号やＭＡＣアドレスなどは、無線機器３に固有の情報として固有情報取得部２１が取得する（ステップＣ２）。

【００４７】また、固有情報取得部２１は、この取得した情報を暗号キー作成部２２に転送する。一方、暗号キー作成部２２は、この転送された情報を利用して、無線機器３が無線通信時に用いる暗号キーを作成する（ステップＣ３）。そして、暗号キー設定部２４は、この暗号キー作成部２２が作成した暗号キーを自装置のパーソナルコンピュータ２に設定する（ステップＣ４）。

【００４８】さらに、暗号キー設定指示部２３は、この暗号キー作成部２２が作成した暗号キーを設定させるための命令を、Ｉ／Ｏコントローラ１０６を介して無線機器３に向けて発行する（ステップＣ５）。一方、この命令をＩ／Ｏコントローラ２０７を介して受け取った無線機器３では、暗号キー設定部３１が、この暗号キーをＥＥＰＲＯＭ２０２に格納する（ステップＣ６）。

【００４９】このように、この実施形態の暗号キー設定システムでは、パーソナルコンピュータ２と無線機器３との各セットごとに、固有の暗号キーを同期させながら簡単に設定することを実現する。

【００５０】なお、前述した実施形態では、IEEE802.11を例に説明したが、これに限定されず、本願発明は、たとえばIEEE802.11aにも適用可能である。

【００５１】つまり、本願発明は、前記実施形態に限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。更に、前記

実施形態には種々の段階の発明が含まれており、開示される複数の構成要件における適宜な組み合わせにより種々の発明が抽出され得る。たとえば、実施形態に示される全構成要件から幾つかの構成要件が削除されても、発明が解決しようとする課題の欄で述べた課題が解決でき、発明の効果の欄で述べられている効果が得られる場合には、この構成要件が削除された構成が発明として抽出され得る。

【００５２】

【発明の効果】以上、詳述したように、この発明によれば、たとえば製造・販売元からの出荷時などにおいて、製造番号やＭＡＣ（Media Access Control）アドレスなど、無線通信装置に固有の情報を取得し、その固有情報から暗号キーを作成して、それぞれの無線通信装置に設定するため、ユーザが出荷時と同じ初期設定のままの状態で無線通信装置を使い始めたとしても、無関係な相手との通信が行われてしまうといった事態を防止し、セキュリティを維持することを実現する。

【図面の簡単な説明】

【図１】この発明の第１実施形態に係る暗号キー設定システムの全体図。

【図２】同第１実施形態のパーソナルコンピュータの機器構成を示す図。

【図３】同第１実施形態の無線機器の機器構成を示す図。

【図４】同第１実施形態の暗号キー設定システムの動作手順を示すフローチャート。

【図５】同第２実施形態に係る暗号キー設定システムの全体図。

【図６】同第２実施形態の暗号キー設定システムの動作手順を示すフローチャート。

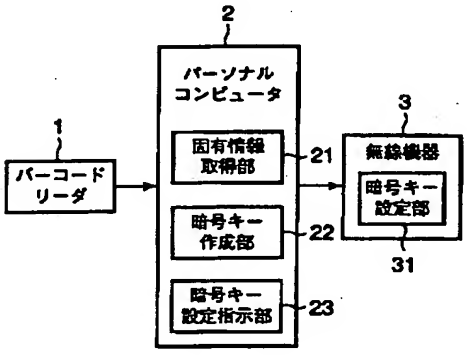
【図７】同第３実施形態に係る暗号キー設定システムの全体図。

【図８】同第３実施形態の暗号キー設定システムの動作手順を示すフローチャート。

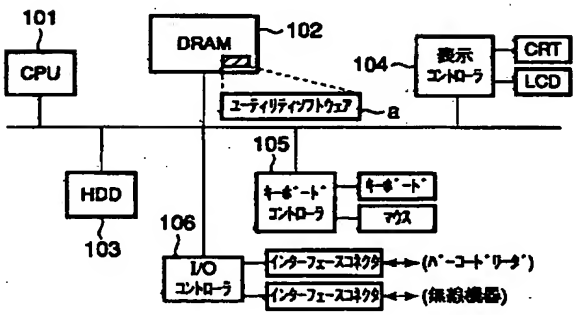
【符号の説明】

１…バーコードリーダ
２…パーソナルコンピュータ
３…無線機器
２１…固有情報取得部
２２…暗号キー作成部
２３…暗号キー設定指示部
２４…（パーソナルコンピュータ側）暗号キー設定部
３１…（無線機器側）暗号キー設定部
３２…暗号キー作成部
１０１…ＣＰＵ
１０２…ＤＲＡＭ
１０３…ＨＤＤ
１０４…表示コントローラ
１０５…キーボードコントローラ
１０６…Ｉ／Ｏコントローラ
２０１…ＣＰＵ
２０２…ＥＥＰＲＯＭ
２０３…フラッシュメモリ
２０４…ＤＲＡＭ
２０５…無線通信部
２０６…表示コントローラ
２０７…Ｉ／Ｏコントローラ
ａ…ユーティリティソフトウェア
ｂ…暗号キー
ｃ…暗号キー設定プログラム

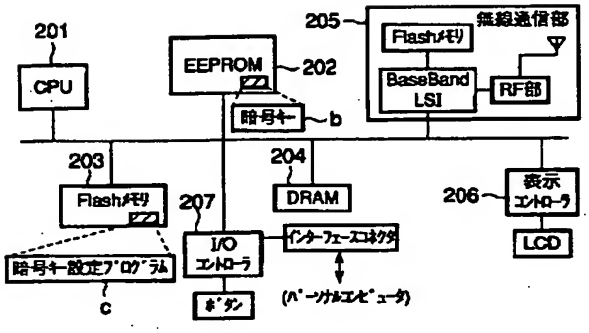
【図１】



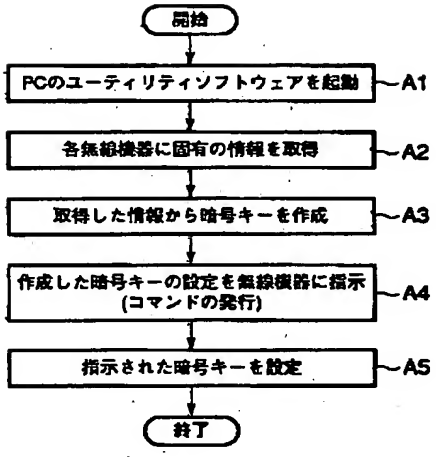
【図２】



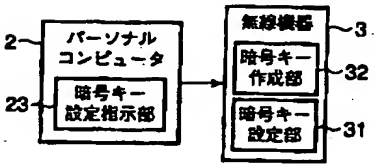
【図３】


201
CPU
EEPROM
202
暗号キー
b
205
無線通信部
Flashメモリ
BaseBand LSI
RF部
203
Flashメモリ
204
DRAM
207
I/O コントローラ
インターフェースコネクタ
206
表示コントローラ
LCD
暗号キー設定プログラム
c
ボタン
(パーソナルコンピュータ)

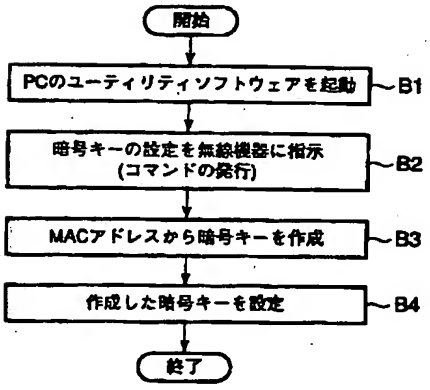
【図４】


開始
PCのユーティリティソフトウェアを起動
A1
各無線機器に固有の情報を取得
A2
取得した情報から暗号キーを作成
A3
作成した暗号キーの設定を無線機器に指示 (コマンドの発行)
A4
指示された暗号キーを設定
A5
終了

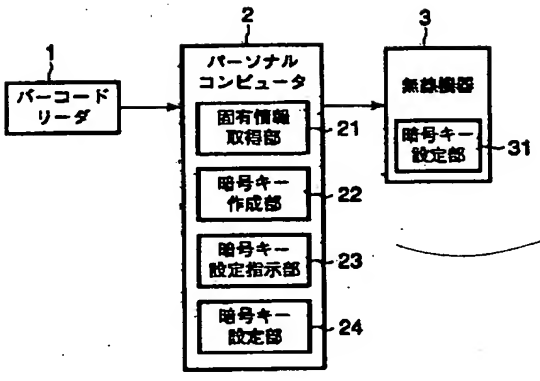
【図５】


2
パーソナルコンピュータ
23
暗号キー設定指示部
無線機器
3
暗号キー作成部
32
暗号キー設定部
31

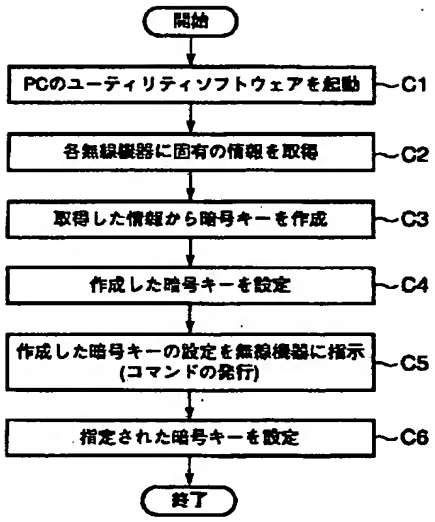
【図６】


開始
PCのユーティリティソフトウェアを起動
B1
暗号キーの設定を無線機器に指示 (コマンドの発行)
B2
MACアドレスから暗号キーを作成
B3
作成した暗号キーを設定
B4
終了

【図７】


1
バーコードリーダ
2
パーソナルコンピュータ
固有情報取得部
21
暗号キー作成部
22
暗号キー設定指示部
23
暗号キー設定部
24
3
無線機器
暗号キー設定部
31

【図８】


開始
PCのユーティリティソフトウェアを起動
C1
各無線機器に固有の情報を取得
C2
取得した情報から暗号キーを作成
C3
作成した暗号キーを設定
C4
作成した暗号キーの設定を無線機器に指示
(コマンドの発行)
C5
指定された暗号キーを設定
C6
終了